(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 2 863 578 A1

(12) EUROPEAN PATENT APPLICATION
published in accordance with Art. 153(4) EPC

(43) Date of publication:
22.04.2015 Bulletin 2015/17

(21) Application number: **13804786.5**

(22) Date of filing: **28.05.2013**

(51) Int Cl.:
H04L 9/32 *(2006.01)* ***H04L 9/08*** *(2006.01)*

(86) International application number:
PCT/CN2013/076315

(87) International publication number:
WO 2013/185531 (19.12.2013 Gazette 2013/51)

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR
Designated Extension States:
BA ME

(30) Priority: **14.06.2012 CN 201210195842**

(71) Applicant: **ZTE Corporation**
Shenzhen, Guangdong 518057 (CN)

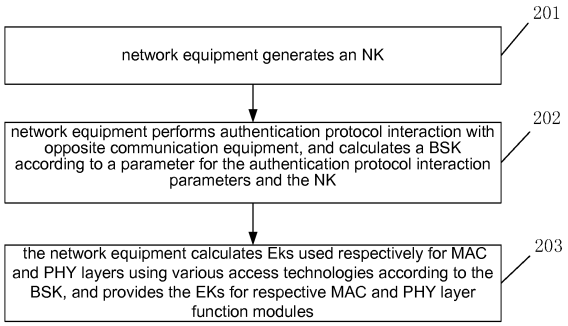
(72) Inventors:
- **LIANG, Qiongwen**
  Shenzhen
  Guangdong 518057 (CN)
- **ZHANG, Weiliang**
  Shenzhen
  Guangdong 518057 (CN)
- **WANG, Lin**
  Shenzhen
  Guangdong 518057 (CN)
- **ZHANG, Junjian**
  Shenzhen
  Guangdong 518057 (CN)
- **ZHANG, Dezhi**
  Shenzhen
  Guangdong 518057 (CN)
- **ZHANG, Boshan**
  Shenzhen
  Guangdong 518057 (CN)

(74) Representative: **Wilson Gunn**
Blackfriars House
The Parsonage
5th Floor
Manchester M3 2JA (GB)

(54) NETWORK DEVICE AND AUTHENTICATION THEREOF AND KEY MANAGEMENT METHOD

(57) Provided is a network equipment and an authentication and key management method for the same. The network equipment generates a Network Key (NK); the network equipment performs authentication protocol interaction with opposite communication equipment, and calculates a Basic Session Key (BSK) according to parameters for the authentication protocol interaction and the NK; and the network equipment calculates link Encryption Keys (EKs) used respectively for Media Access Control (MAC) and Physical (PHY) layers using various access technologies according to the BSK, and provides the EKs for respective MAC and PHY layer function modules. With the disclosure, the legality of the equipment is verified by performing an authentication process on the heterogeneous network equipments in one pass, and keys in various MAC layer technologies are managed in a unified way.

Fig. 2



EP 2 863 578 A1

Description

TECHNICAL FIELD

[0001] The disclosure relates to a heterogeneous network convergence technology, in particular to a network equipment and an authentication and key management method for the same.

BACKGROUND

[0002] At present, a home network can be accessed by virtue of multiple network technologies, for example: Ethernet Institute of Electrical and Electronics Engineers (IEEE) 802.3, Power Line Communication (PLC), Multimedia over Coax Alliance (MoCA) and a Wireless Fidelity (WiFi) technology, and each access technology corresponds to a Physical (PHY) layer and a Media Access Control (MAC) layer of a network system model. The convergence of the heterogeneous network technologies is a basis for realizing the information sharing and seamless connection of the home network.

[0003] Fig. 1 is a structure diagram of heterogeneous network convergence in prior art. As shown in Fig. 1, equipment 1 and equipment 2 are home network equipments using three MAC layer and PHY layer access technologies. Each network access technology uses a different communication media, media control access mode, transmission frame format and the like from those used by another network access technology, so that technologies for PHY layers and MAC layers of corresponding network systems are different from each other. Therefore, when multiple network access technologies are implemented on one equipment, a convergence control module is required to realize the coordination and scheduling of various MAC layer and PHY layer technologies to realize seamless technical convergence. Each equipment corresponds to a convergence control module, and each convergence control module can coordinate and manage at least two MAC layer and PHY layer function modules.

[0004] At present, the most common security configuration for home networking is implemented by inputting a password to a network equipment by a user, and although there is security configuration supporting user password input in the MAC layer technologies such as PLC, MoCA and WiFi, authentication and key management processes in various MAC layer technologies process the user password input procedure differently, which causes the non-interworking of various security management processes. For example, assuming that the equipment 1 and the equipment 2 in Fig. 1 are configured with a same user password, if the two equipments are connected only through a PLC link, the equipments process the user password according to an authentication and key negotiation process of the PLC, and calculate a link Encryption Key (EK) of the PLC; and if the equipment 1 and the equipment 2 are connected by virtue of three MAC layer technologies, the two equipments have to use the user password to perform authentication and key negotiation processes specified by the three MAC layer technologies, so as to obtain link EKs of the three links respectively. That is, the security authentication and key management process in the prior art is performed for each MAC layer interface on the network equipment rather than for the equipment itself; and authentication and key management methods for each MAC layer technology are different from one another, so that the authentication and key negotiation process specified by each MAC layer technology has to be performed when the network equipment is connected by virtue of multiple MAC layer technologies, which inevitably causes calculation resource waste in an authentication process.

SUMMARY

[0005] An embodiment of the disclosure provides a network equipment and an authentication and key management method for the same, for avoid calculation resource waste in an authentication execution process caused by applying different authentication and key management methods for various MAC layer technologies in the prior art.

[0006] In view of the above, the embodiment of the disclosure is implemented as follows:

the embodiment of the disclosure provides an authentication and key management method for network equipment, the method including that:

the network equipment generates a Network Key (NK);

the network equipment performs authentication protocol interaction with opposite communication equipment, and calculates a Basic Session Key (BSK) according to authentication protocol interaction parameters and the NK; and

the network equipment calculates link EKs used for MAC and PHY layers using various access technologies according to the BSK, and provides the respective EKs for respective MAC and PHY layer function modules.

[0007] Preferably, the network equipment generates the NK according to an acquired password, or the network equipment generates the NK by using a WPS Push-Button function in a wireless local network WiFi.

[0008] Preferably, after the EKs are provided for the respective MAC and PHY layer function modules, the method further includes that:

the MAC and PHY layer function modules perform encryption and decryption protection on the data communicated between the network equipment and

the opposite communication equipment according to the acquired EKs.

[0009] Preferably, before the network equipment generates the NK according to the acquired password, the method further includes that:

the network equipment and the opposite communication equipment interact about equipment capability information, and after both the network equipment and the opposite communication equipment are confirmed to support a specific authentication and key management function, subsequent processing operation is performed.

[0010] Preferably, the step that the network equipment calculates the link EKs used respectively for the MAC and PHY layers using various access technologies according to the BSK, and provides the EKs for the respective MAC and PHY layer function modules includes that:

the BSK is input into a key deduction algorithm implemented by a hash function for calculation, and the EKs with respective lengths are output to the respective MAC and PHY layer function modules according to the EK lengths required by the MAC and PHY layers using various access technologies.

[0011] Preferably, the MAC and PHY layers using various access technologies include:

MAC and PHY layers using PLC;

MAC and PHY layers using MoCA; and

MAC and PHY layers using WiFi.

[0012] Preferably, the authentication protocol interaction parameters include: a convergence control module Identifier (ID) of the network equipment, a Random Number (RN) selected by the network equipment, a convergence control module ID of the opposite communication equipment and an RN selected by the opposite communication equipment;
the convergence control module ID of the network equipment is a MAC address of a convergence control module of the network equipment, or a MAC address which uniquely identifies the identity of the network equipment; and
the convergence control module ID of the opposite communication equipment is a MAC address of a convergence control module of the opposite communication equipment, or a MAC address which uniquely identifies the identity of the opposite communication equipment.

[0013] Preferably, the BSK includes: a unicast BSK and/or a multicast BSK;
accordingly, the method further includes that:

the network equipment calculates unicast EKs according to the unicast BSK, and calculates multicast EKs according to the multicast BSK; and

the MAC and PHY layer function modules of the network equipment perform encryption and decryption protection on unicast data according to the unicast EKs, and perform encryption and decryption protection on multicast data according to the multicast EKs.

[0014] The embodiment of the disclosure also provides network equipment, which includes: a convergence control module and MAC and PHY layer function modules using various access technologies, wherein
the convergence control module is configured to generate an NK, and is further configured to perform authentication protocol interaction between the network equipment and opposite communication equipment, calculate a BSK according to parameters for authentication protocol interaction and the NK, calculate link EKs used respectively for MAC and PHY layers using various access technologies and provide the EKs for the respective MAC and PHY layer function modules; and
the MAC and PHY layer function modules are configured to receive the respective EKs provided by the convergence control module.

[0015] Preferably, the convergence control module generates the NK according to an acquired password, or generates the NK by using a WPS Push-Button function in a wireless local network WiFi.

[0016] Preferably, the MAC and PHY layer function modules are further configured to perform encryption and decryption protection on the data communicated between the network equipment and the opposite communication equipment according to the acquired EKs.

[0017] Preferably, the convergence control module is further configured to, before generating the NK according to the acquired password, interact with the opposite communication equipment about equipment capability information, and after both the network equipment and the opposite communication equipment are confirmed to support a specific authentication and key management function, perform subsequent processing operation.

[0018] Preferably, the convergence control module is further configured to input the BSK into a key deduction algorithm implemented by a hash function for calculation and output the EKs with respective lengths to the respective MAC and PHY layer function modules according to the EK lengths required by the MAC and PHY layers using various access technologies.

[0019] Preferably, the MAC and PHY layers using various access technologies include:

MAC and PHY layers using PLC;

MAC and PHY layers using MoCA; and

MAC and PHY layers using WiFi.

[0020] Preferably, the authentication protocol interaction parameters include: a convergence control module ID of the network equipment, an RN selected by the network equipment, a convergence control module ID of the opposite communication equipment and an RN selected by the opposite communication equipment;
the convergence control module ID of the network equipment is a MAC address of the convergence control module of the network equipment, or a MAC address which uniquely identifies the identity of the network equipment; and
the convergence control module ID of the opposite communication equipment is a MAC address of a convergence control module of the opposite communication equipment, or a MAC address which uniquely identifies the identity of the opposite communication equipment.

[0021] Preferably, the BSK includes: a unicast BSK and/or a multicast BSK;
accordingly, convergence control module is further configured to calculate unicast EKs according to the unicast BSK and calculate multicast EKs according to the multicast BSK; and
the MAC and PHY layer function modules are further configured to perform encryption and decryption protection on unicast data according to the unicast EKs and perform encryption and decryption protection on multicast data according to the multicast EKs.

[0022] According to the network equipment and the authentication and key management method for the same provided by the embodiment of the disclosure, legality authentication between a network and equipment and between equipment and equipment can be implemented only by executing a unified authentication protocol flow once by the convergence control module of the network equipment without executing various authentication protocol flows of the MAC and PHY layers by virtue of the password input by a user by the multiple MAC and PHY layer function modules on the network equipment, so that a calculation resource in an authentication process is saved. In addition, keys in various MAC and PHY layer technologies are managed in a unified way, and a data encryption and decryption manner used by various MAC and PHY layer function modules can be kept unchanged, so that cost in the upgrading of such a function of the equipment will be reduced.

BRIEF DESCRIPTION OF THE DRAWINGS

[0023]

Fig. 1 is a structure diagram of heterogeneous network convergence in prior art;

Fig. 2 is a flowchart of an authentication and key management method for a network equipment according to embodiment 1 of the disclosure;

Fig. 3 is a flowchart of an authentication and key management method for a network equipment according to embodiment 2 of the disclosure;

Fig. 4 is a flowchart of an authentication and key management method for a network equipment according to embodiment 3 of the disclosure;

Fig. 5 is a flowchart of equipment capability information interaction according to an embodiment of the disclosure; and

Fig. 6 is a flowchart of authentication protocol interaction according to an embodiment of the disclosure.

DETAILED DESCRIPTION

[0024] The technical solution of the disclosure is further described below with reference to the drawings and specific embodiments in detail.

[0025] As shown in Fig. 2, an authentication and key management method for a network equipment according to embodiment 1 of the disclosure mainly includes the following steps:

Step 201: the network equipment generates an NK.

[0026] The network equipment can generate the NK according to an acquired password. Specifically, a user inputs the password at a user interface of the network equipment, a length of the password not exceeding a maximum length set by the user interface, and the network equipment inputs the password input by the user to a pseudo-random function for calculation, so as to acquire the NK with a fixed length.

[0027] Besides acquiring the NK by the user inputting the password, if the network equipment has a simple security configuration function according to an implementation specification for simple WiFi configuration, the network equipment may generate the NK by using a WPS Push-Button function in WiFi.

[0028] Specifically, if the network equipments of both the communication parties have WPS Push-Button functions and a communication protocol function specified in the simple configuration specification for WiFi, the two network equipments can interact with each other according to the communication protocol specified in the simple configuration specification for WiFi by pressing the WPS Push-Button functions on the two network equipments within a specific time interval (for example, 2 minutes) after the network equipments are connected through certain physical medium. After the protocol is successfully performed, the two network equipment can acquire the NK with the fixed length.

[0029] Step 202: the network equipment performs authentication protocol interaction with opposite communication equipment, and calculates a BSK according to parameters for the authentication protocol interaction and the NK.

[0030] The network equipment inputs the parameters for authentication protocol interaction and the NK into a hash function to calculate the BSK.

[0031] Authentication may be the authentication of a network side over the network equipment, and also may be the authentication of network equipment over network equipment; and if the authentication is the authentication of the network side over the network equipment, the opposite communication equipment is authentication equipment on the network side, and if the authentication is the authentication of the network equipment over the network equipment, the opposite communication equipment is another network equipment.

[0032] An authentication protocol interaction process is performed by convergence control modules of the network equipment and the opposite communication equipment, and will be specifically described in the subsequent embodiment in detail.

[0033] Step 203: the network equipment calculates link EKs used respectively for MAC and PHY layers using various access technologies according to the BSK, and provides the EKs for respective MAC and PHY layer function modules.

[0034] In the embodiment, the MAC and PHY layers using various access technologies at least include: MAC and PHY layers using PLC, MAC and PHY layers using MoCA, MAC and PHY layers using WiFi and the like.

[0035] The convergence control module of the network equipment inputs the BSK into a key deduction algorithm implemented by the hash function for calculation, and outputs the EKs with respective lengths to the respective MAC and PHY layer function modules according to the EK lengths required by the MAC and PHY layers using various access technologies. Wherein, the key deduction algorithm implemented by the hash function can output keys with enough lengths, and if it is supposed that a key length required by the MAC and PHY layers using PLC is m, a key length required by the MAC and PHY layers using WiFi is n and a key length required by the MAC and PHY layers using MoCA is t, the key deduction algorithm implemented by the hash function can output a key with a length x which should be greater than or equal to a maximum numerical value in m, n and t.

[0036] The convergence control module outputs the EKs with the respective lengths according to the key lengths required by specific MAC and PHY layers, and the specific MAC and PHY layers may be the MAC and PHY layers using WiFi, or the MAC and PHY layers using MoCA or the MAC and PHY layers using PLC. The length x of the key output by the key deduction algorithm implemented by the hash function is greater than or equal to the maximum numerical value in m, n and t, so that the convergence control module is required to extract a part (which can be extracted from any position of a key string) with a length n from the key string with a length x as the EK of the specific MAC and PHY layers for output if it is supposed that the key length n required by the specific MAC and PHY layers is smaller than x. The convergence control module transmits the output EK to specific MAC and PHY layer function modules. For example, if the length of the key string generated by the key deduction algorithm implemented by the hash function is 512 bits and the key length required by the MAC and PHY layers using PLC is 256 bits, the former 256 bits are extracted from the key string as the EK for the MAC and PHY layers using PLC; and the convergence control module outputs the extracted 256-bit EK to the MAC and PHY layer function modules using PLC.

[0037] As a preferred embodiment, as shown in Fig. 3, after the Step 203, Step 204 can also be performed: the MAC and PHY layer function modules perform encryption and decryption protection on the data of communication between the network equipment and the opposite communication equipment. Specifically, the MAC and PHY layer function modules store and install the acquired EKs, and subsequently perform encryption and decryption protection on the data of communication between the network equipment and the opposite communication equipment by using the installed EKs. For example: the MAC and PHY layer function modules using PLC acquire the EKs which are output by the convergence control module and correspond to the MAC and PHY layers using PLC, the MAC and PHY layer function modules using MoCA acquire the EKs which are output by the convergence control module and correspond to the MAC and PHY layers using MoCA, and the MAC and PHY layer function modules using WiFi acquire the EKs which are output by the convergence control module and correspond to the MAC and PHY layers using WiFi.

[0038] It should be noted that the BSK in the embodiment of the disclosure includes: a unicast BSK and/or a multicast BSK; correspondingly, the network equipment calculates unicast EKs according to the unicast BSK, and calculates multicast EKs according to the multicast BSK; and the MAC and PHY layer function modules of the network equipment perform encryption and decryption protection on unicast data according to the unicast EKs, and perform encryption and decryption protection on multicast data according to the multicast EKs.

[0039] As another preferred embodiment of the disclosure, as shown in Fig. 4, before Step 201, Step 200 can also be performed: the network equipment and the opposite communication equipment interact about equipment capability information, and only when it is confirmed that both the network equipment and the opposite communication equipment support a specific authentication and key management function (i.e. a function of executing Step 201 to Step 204) in the embodiment of the disclosure, subsequent processing operation (i.e. Step 201 to Step 204) is performed. The interaction about the equipment capability information between equipment A and equipment B is taken as an example, and as shown in Fig. 5, a specific flow mainly includes that:

Step 501: the equipment B initiates an equipment capability request message to the equipment A.

[0040] The equipment capability request message includes whether the equipment B has the specific authentication and key management function in the embodiment of the disclosure or not. For example: if a value of a specific field in the request message is 0, it is indicated that the equipment B does not support the specific authentication and key management function in the embodiment of the disclosure; and if the value of the specific field is 1, it is indicated that the equipment B supports the specific authentication and key management function in the embodiment of the disclosure.

[0041] Step 502: the equipment A transmits an equipment capability response message to the equipment B.

[0042] The equipment capability response message includes whether the equipment A has the specific authentication and key management function in the embodiment of the disclosure or not. For example: if a value of a specific field in the request message is 0, it is indicated that the equipment A does not support the specific authentication and key management function in the embodiment of the disclosure; and if the value of the specific field is 1, it is indicated that the equipment A supports the specific authentication and key management function in the embodiment of the disclosure.

[0043] Only when both the equipment A and the equipment B support the specific authentication and key management function in the embodiment of the disclosure, the operation in the subsequent Step 201 to Step 204 is performed.

[0044] An authentication protocol interaction flow in the embodiment of the disclosure is described below with reference to Fig. 6 in detail, and as shown in Fig. 6, mainly includes the following steps that:

Step 601: the equipment B initiates an authentication request message to the equipment A.

[0045] The authentication request message at least includes: a convergence control module ID (IDB for short) on the equipment B and an RN selected by the equipment B (RNB for short).

[0046] Step 602: the equipment A returns an authentication response message to the equipment B after receiving the authentication request message.

[0047] The authentication response message includes at least: a convergence control module ID (IDA for short) on the equipment A, an RN (RNA for short) selected by the equipment A and a message authentication code for verifying the legality of the authentication response message.

[0048] Step 603: the equipment B returns an authentication confirmation message to the equipment A after receiving the authentication response message.

[0049] The authentication confirmation message at least includes: authentication success or failure status information, the convergence control module IDB on the equipment B and a message authentication code for verifying the legality of the authentication confirmation message.

[0050] Step 604: the equipment A transmits a completion message to the equipment B after receiving the authentication confirmation message returned by the equipment B.

[0051] The completion message includes at least: the authentication success or failure state information and a message authentication code for verifying the legality of the completion message.

[0052] In a specific application, the above involved convergence control module ID can adopt a MAC address of the convergence control module as well as a MAC address which can uniquely identify the identity of the equipment.

[0053] By the above authentication protocol interaction, the equipment A and the equipment B implement network key pre-sharing-based two-way authentication. After successful authentication, the equipment A and the equipment B input the IDB on the equipment B, the IDA on the equipment A, the RNB selected by the equipment B and the RNA selected by the equipment A into the hash function as the authentication protocol interaction parameters in Step 204 together with the NK obtained in Step 203 to calculate the BSK.

[0054] It can be seen that after the same password is input to the network equipment and the opposite communication equipment and the same Step 200 to Step 204 are performed, the MAC and PHY layer function modules, using PLC, of the network equipment and the MAC and PHY layer function modules, using PLC, of the opposite communication equipment can obtain the same EKs, and can perform encryption and decryption protection on the data of communication between the network equipment and the opposite communication equipment according to the EKs; similarly, the MAC and PHY layer function modules, using MoCA, of the network equipment and the MAC and PHY layer function modules, using MoCA, of the opposite communication equipment can also obtain the same EKs, and can perform encryption and decryption protection on the data of communication between the network equipment and the opposite communication equipment according to the EKs; and the MAC and PHY layer function modules, using WiFi, of the network equipment and the MAC and PHY layer function modules, using WiFi, of the opposite communication equipment can obtain the same EKs, and can perform encryption and decryption protection on the data of communication between the network equipment and the opposite communication equipment according to the EKs.

[0055] By the embodiment of the disclosure, legality authentication between a network and equipment and between equipment and equipment can be implemented only by executing a unified authentication protocol flow once by the convergence control module of the network equipment without executing various authentication protocol flows of the MAC and PHY layers by virtue of the password input by the user by the multiple MAC and PHY layer function modules on the network equipment, so that

a calculation resource in an authentication process is saved. In addition, keys in various MAC and PHY layer technologies are managed in a unified way, and a data encryption and decryption manner used by various MAC and PHY layer function modules can be kept unchanged, so that cost in the upgrading of such a function of the equipment will not be high.

[0056] Based on the authentication and key management method, the embodiment of the disclosure also provides network equipment, which includes: a convergence control module and MAC and PHY layer function modules using various access technologies, wherein

the convergence control module is configured to generate an NK, and is further configured to perform authentication protocol interaction between the network equipment and opposite communication equipment, calculate a BSK according to authentication protocol interaction parameters and the NK, calculate EKs used for MAC and PHY layers using various access technologies and provide the EKs for the corresponding MAC and PHY layer function modules respectively; and

the MAC and PHY layer function modules are configured to receive the corresponding EKs provided by the convergence control module.

[0057] The MAC and PHY layers using various access technologies at least include: MAC and PHY layers using PLC; MAC and PHY layers using MoCA; and MAC and PHY layers using WiFi.

[0058] Preferably, the convergence control module can generate the NK according to an acquired password, or generate the NK in a manner of using a WPS Push-Button function in WiFi.

[0059] Preferably, the MAC and PHY layer function modules are further configured to perform encryption and decryption protection on the data communicated between the network equipment and the opposite communication equipment according to the acquired EKs.

[0060] Preferably, the convergence control module is further configured to, before generating the NK according to the acquired password, interact with the opposite communication equipment about equipment capability information, and after both the network equipment and the opposite communication equipment are confirmed to support a specific authentication and key management function, perform subsequent processing operation.

[0061] Preferably, the convergence control module is further configured to input the BSK into a key deduction algorithm implemented by a hash function for calculation and output the EKs with respective lengths to the respective MAC and PHY layer function modules according to the EK lengths required by the MAC and PHY layers using various access technologies.

[0062] The authentication protocol interaction parameters include: a convergence control module ID of the network equipment, an RN selected by the network equipment, a convergence control module ID of the opposite communication equipment and an RN selected by the opposite communication equipment;

the convergence control module ID of the network equipment is a MAC address of the convergence control module of the network equipment, or a MAC address which uniquely identifies the identity of the network equipment; and

the convergence control module ID of the opposite communication equipment is a MAC address of a convergence control module of the opposite communication equipment, or a MAC address which uniquely identifies the identity of the opposite communication equipment.

[0063] Preferably, the BSK includes: a unicast BSK and/or a multicast BSK;

accordingly, convergence control module is further configured to calculate unicast EKs according to the unicast BSK and calculate multicast EKs according to the multicast BSK; the same method is adopted for calculating the unicast EKs according to the unicast BSK and calculating the multicast EKs according to the multicast BSK; and

the MAC and PHY layer function modules are further configured to perform encryption and decryption protection on unicast data according to the unicast EKs and perform encryption and decryption protection on multicast data according to the multicast EKs.

[0064] If the modules in the embodiment of the disclosure are implemented in a form of a software function module, and are sold or used as independent products, the modules can also be stored in a computer-readable storage medium. Based on such understanding, the technical solution of the embodiment of the disclosure itself or a part contributing to the prior art can be embodied in a form of a software product, and the computer software product is stored in a storage medium, and includes multiple instructions configured to enable a piece of computer equipment (which may be a personal computer, a server, network equipment or the like) to perform all or a part of the method in each embodiment of the disclosure. The storage medium includes various media capable of storing program codes, such as: a Universal Serial Bus (USB) flash disk, a mobile hard disk drive, a Read-Only Memory (ROM), a Random Access Memory (RAM), a magnetic disk or an optical disc. Therefore, the embodiment of the disclosure is not limited to any specific hardware and software combination.

[0065] Accordingly, the embodiment of the disclosure also provides a computer storage medium, in which a computer program is stored, wherein the computer program is configured to perform an authentication and key management method in the embodiment of the disclosure.

[0066] The above is only the preferred embodiment of the disclosure and not intended to limit the scope of protection of the disclosure.

Claims

1. An authentication and key management method for

a network equipment, comprising:

generating, by the network equipment, a Network Key (NK);
performing, by the network equipment, authentication protocol interaction with an opposite communication equipment, and calculating a Basic Session Key (BSK) according to parameters for the authentication protocol interaction and the NK; and
calculating, by the network equipment, link Encryption Keys (EKs) used respectively for a Media Access Control (MAC) layer and a Physical (PHY) layer using various access technologies according to the BSK, and providing the EKs for the respective MAC and PHY layer function modules.

2. The authentication and key management method for the network equipment according to claim 1, wherein the network equipment generates the NK according to an acquired password, or the network equipment generates the NK by using a WPS Push-Button function in a wireless local network Wireless Fidelity (WiFi).

3. The authentication and key management method for the network equipment according to claim 1, further comprising:

after providing the EKs for the respective MAC and PHY layer function modules,
performing, by the MAC and PHY layer function modules, encryption and decryption protection on data communicated between the network equipment and the opposite communication equipment according to the acquired EKs.

4. The authentication and key management method for the network equipment according to claim 1, 2 or 3, further comprising:

before generating, by the network equipment, the NK according to the acquired password,
performing, by the network equipment and the opposite communication equipment, interaction about equipment capability information, and
performing subsequent processing operation, only after both the network equipment and the opposite communication equipment are confirmed to support a specific authentication and key management function,.

5. The authentication and key management method for the network equipment according to claim 1, 2 or 3, wherein calculating, by the network equipment, the link EKs used respectively for the MAC layer and the PHY layer using various access technologies according to the BSK, and providing the EKs for the respectively MAC and PHY layer function modules comprises:

inputting the BSK into a key deduction algorithm implemented by a hash function for calculation, and
outputting the EKs with respective lengths to the respective MAC and PHY layer function modules, according to EK lengths required by the MAC and PHY layers using various access technologies.

6. The authentication and key management method for the network equipment according to claim 1, 2 or 3, wherein the MAC and PHY layers using various access technologies comprise:

MAC and PHY layers using Power Line Communication (PLC);
MAC and PHY layers using Multimedia over Coax Alliance (MoCA); and
MAC and PHY layers using WiFi.

7. The authentication and key management method for the network equipment according to claim 1, 2 or 3, wherein the parameters for the authentication protocol interaction comprise: convergence control module Identifier (ID) of the network equipment, Random Number (RN) selected by the network equipment, convergence control module ID of the opposite communication equipment and RN selected by the opposite communication equipment;
the convergence control module ID of the network equipment is MAC address of a convergence control module of the network equipment, or MAC address which uniquely identifies the identity of the network equipment; and
the convergence control module ID of the opposite communication equipment is MAC address of a convergence control module of the opposite communication equipment, or MAC address which uniquely identifies the identity of the opposite communication equipment.

8. The authentication and key management method for the network equipment according to claim 1, 2 or 3, wherein the BSK comprises: a unicast BSK and/or a multicast BSK;
accordingly, the method further comprises:

calculating, by the network equipment, unicast EKs according to the unicast BSK, and calculating multicast EKs according to the multicast BSK; and
performing, by the MAC and PHY layer function modules of the network equipment, encryption and decryption protection on unicast data ac-

cording to the unicast EKs, and performing encryption and decryption protection on multicast data according to the multicast EKs.

9. A network equipment, comprising: a convergence control module and Media Access Control (MAC) and Physical (PHY) layer function modules using various access technologies,
wherein the convergence control module is configured to generate a Network Key (NK), and is further configured to perform authentication protocol interaction between the network equipment and opposite communication equipment, calculate a Basic Session Key (BSK) according to parameters for the authentication protocol interaction and the NK, calculate link Encryption Keys (EKs) used respectively for MAC and PHY layers using various access technologies and provide the EKs for the respective MAC and PHY layer function modules; and
wherein MAC and PHY layer function modules are configured to receive the corresponding EKs provided by the convergence control module.

10. The network equipment according to claim 9, wherein the convergence control module generates the NK according to an acquired password, or generates the NK by using a WPS Push-Button function in a wireless local network Wireless Fidelity (WiFi).

11. The network equipment according to claim 9, wherein the MAC and PHY layer function modules are further configured to perform encryption and decryption protection on the data communicated between the network equipment and the opposite communication equipment according to the acquired EKs.

12. The network equipment according to claim 9, 10 or 11, wherein the convergence control module is further configured to, before generating the NK according to the acquired password,
interact with the opposite communication equipment about equipment capability information, and
perform subsequent processing operation, only after both the network equipment and the opposite communication equipment are confirmed to support a specific authentication and key management function.

13. The network equipment according to claim 9, 10 or 11, wherein the convergence control module is further configured to input the BSK into a key deduction algorithm implemented by a hash function for calculation and output the EKs with respective lengths to the respective MAC and PHY layer function modules according to the EK lengths required by the MAC and PHY layers using various access technologies.

14. The network equipment according to claim 9, 10 or 11, wherein the MAC and PHY layers using various access technologies comprise:

MAC and PHY layers using Power Line Communication (PLC);
MAC and PHY layers using Multimedia over Coax Alliance (MoCA); and
MAC and PHY layers using WiFi.

15. The network equipment according to claim 9, 10 or 11, wherein the parameters for the authentication protocol interaction comprise: convergence control module Identifier (ID) of the network equipment, Random Number (RN) selected by the network equipment, convergence control module ID of the opposite communication equipment and RN selected by the opposite communication equipment;
the convergence control module ID of the network equipment is MAC address of the convergence control module of the network equipment, or MAC address which uniquely identifies the identity of the network equipment; and
the convergence control module ID of the opposite communication equipment is MAC address of a convergence control module of the opposite communication equipment, or MAC address which uniquely identifies the identity of the opposite communication equipment.

16. The network equipment according to claim 9, 10 or 11, wherein the BSK comprises: a unicast BSK and/or a multicast BSK;
accordingly, the convergence control module is further configured to calculate unicast EKs according to the unicast BSK and calculate multicast EKs according to the multicast BSK; and
the MAC and PHY layer function modules are further configured to perform encryption and decryption protection on unicast data according to the unicast EKs and perform encryption and decryption protection on multicast data according to the multicast EKs.

Fig. 1

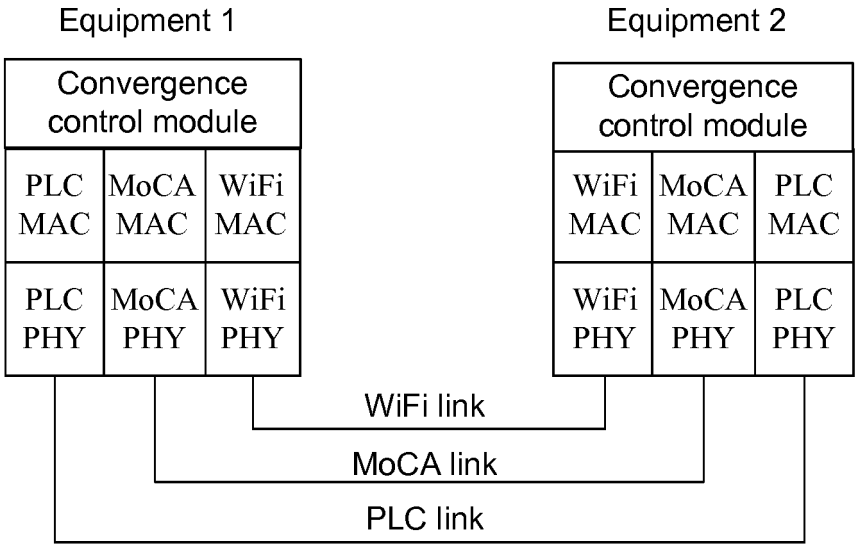

Equipment 1
Equipment 2
Convergence control module
PLC MAC
MoCA MAC
WiFi MAC
PLC PHY
MoCA PHY
WiFi PHY
Convergence control module
WiFi MAC
MoCA MAC
PLC MAC
WiFi PHY
MoCA PHY
PLC PHY
WiFi link
MoCA link
PLC link

Fig. 2

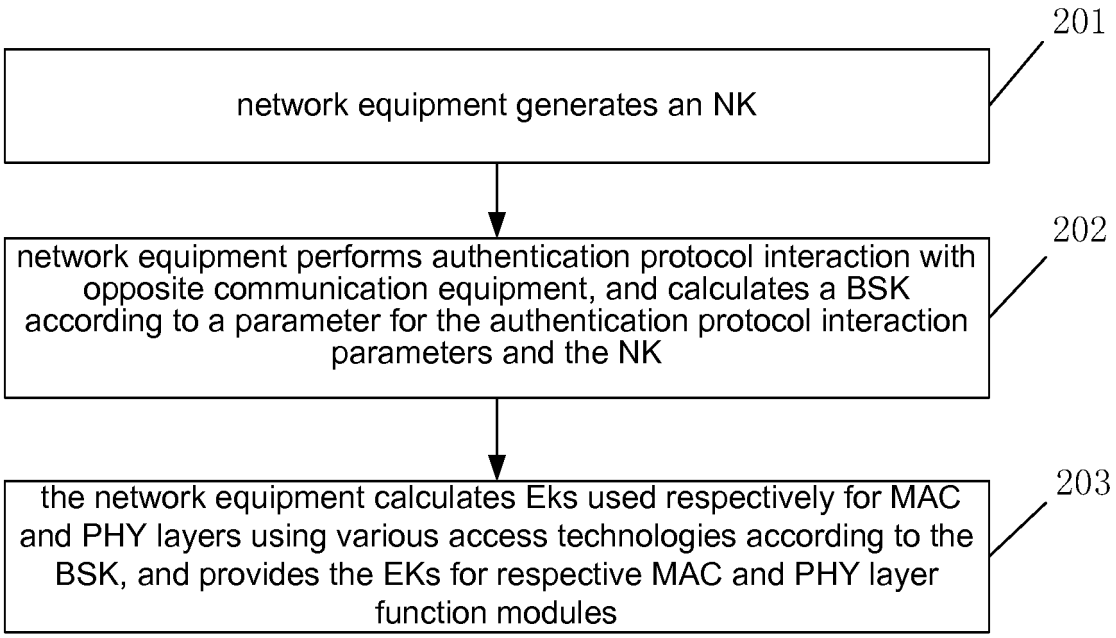

201
network equipment generates an NK
202
network equipment performs authentication protocol interaction with opposite communication equipment, and calculates a BSK according to a parameter for the authentication protocol interaction parameters and the NK
203
the network equipment calculates Eks used respectively for MAC and PHY layers using various access technologies according to the BSK, and provides the EKs for respective MAC and PHY layer function modules

Fig. 3

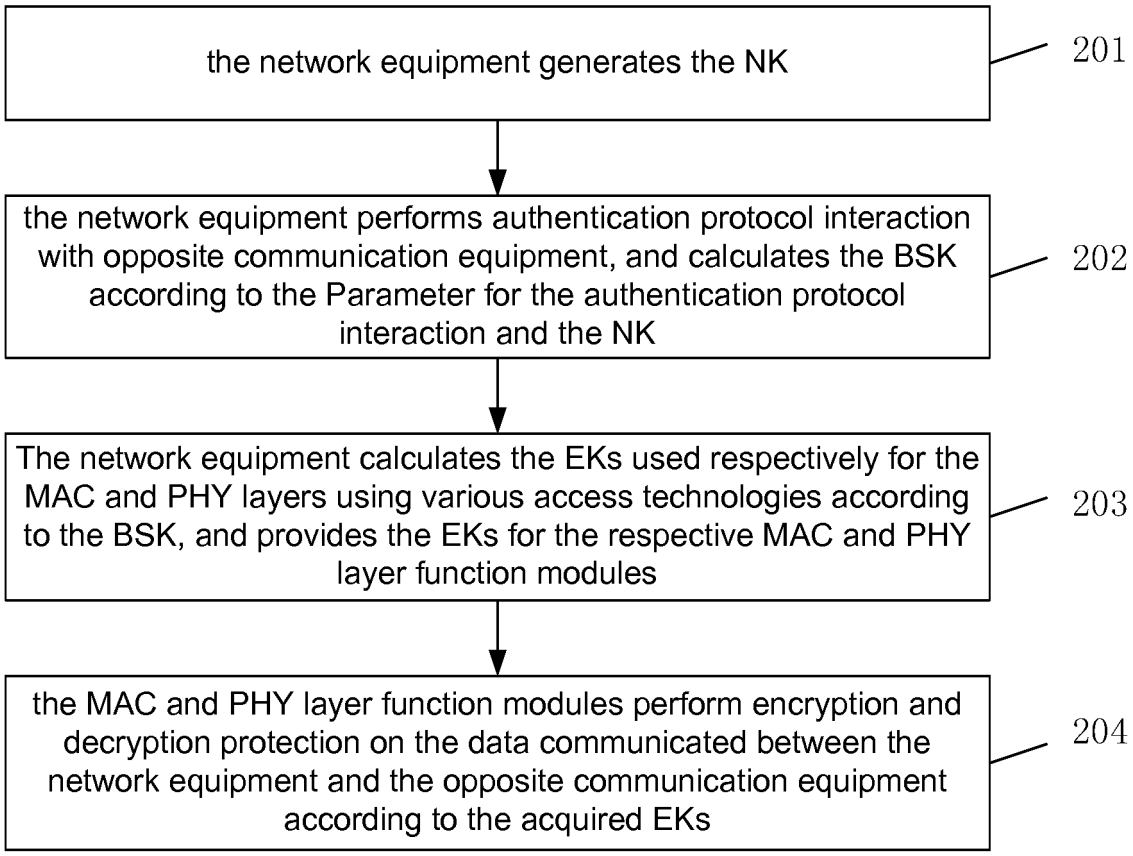

the network equipment generates the NK
201
the network equipment performs authentication protocol interaction with opposite communication equipment, and calculates the BSK according to the Parameter for the authentication protocol interaction and the NK
202
The network equipment calculates the EKs used respectively for the MAC and PHY layers using various access technologies according to the BSK, and provides the EKs for the respective MAC and PHY layer function modules
203
the MAC and PHY layer function modules perform encryption and decryption protection on the data communicated between the network equipment and the opposite communication equipment according to the acquired EKs
204

Fig. 4

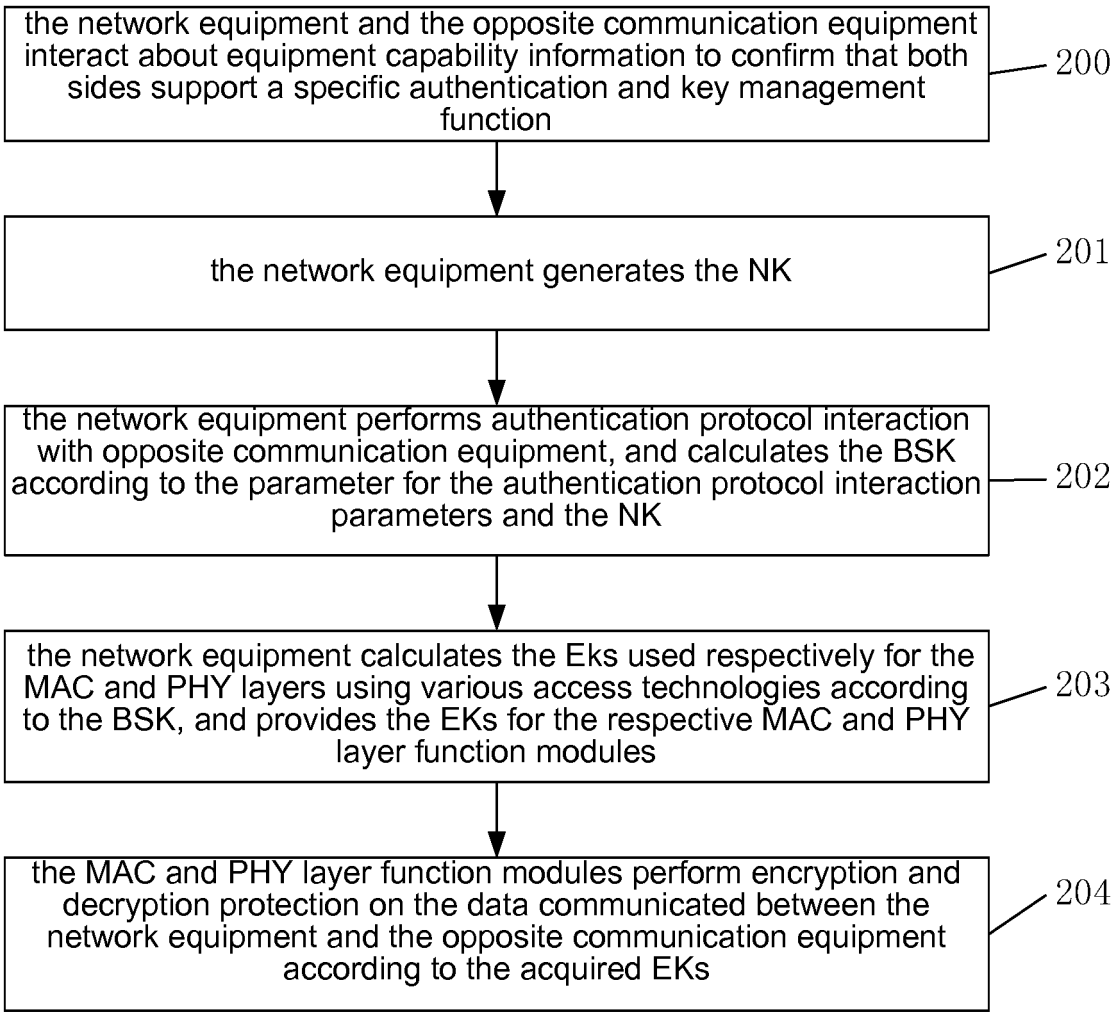

the network equipment and the opposite communication equipment interact about equipment capability information to confirm that both sides support a specific authentication and key management function
200
the network equipment generates the NK
201
the network equipment performs authentication protocol interaction with opposite communication equipment, and calculates the BSK according to the parameter for the authentication protocol interaction parameters and the NK
202
the network equipment calculates the Eks used respectively for the MAC and PHY layers using various access technologies according to the BSK, and provides the EKs for the respective MAC and PHY layer function modules
203
the MAC and PHY layer function modules perform encryption and decryption protection on the data communicated between the network equipment and the opposite communication equipment according to the acquired EKs
204

Fig. 5

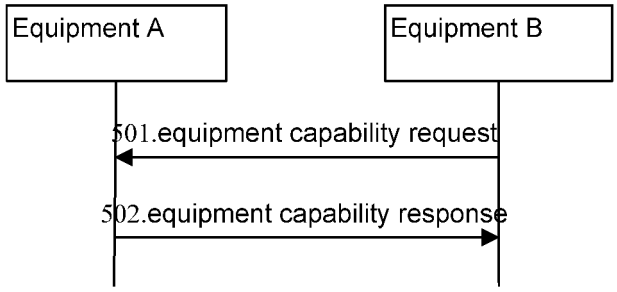
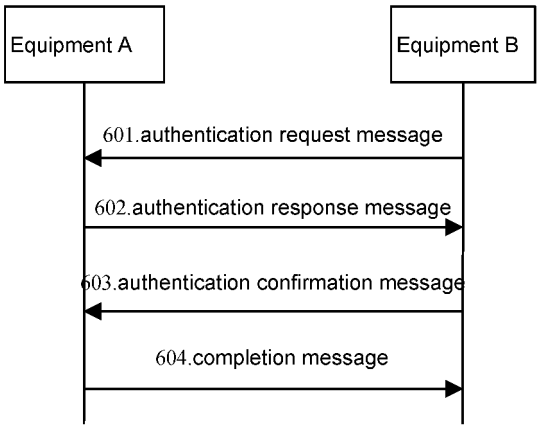

Equipment A
Equipment B
501.equipment capability request
502.equipment capability response

Fig. 6


Equipment A
Equipment B
601.authentication request message
602.authentication response message
603.authentication confirmation message
604.completion message

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/076315

A. CLASSIFICATION OF SUBJECT MATTER

See the extra sheet

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC: H04L, H04W

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI, EPODOC, CNPAT, CNKI: password, MAC, PHY, key, authentication, network equipment, generation, encryption, layer, multi, unity, common, access

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	CN 101516090 A (HUAWEI TECHNOLOGIES CO., LTD.), 26 August 2009 (26.08.2009), description, page 3, line 15 to page 4, line 6	1-16
A	CN 101141241 A (HUAWEI TECHNOLOGIES CO., LTD.), 12 March 2008 (12.03.2008), the whole document	1-16
A	CN 101068143 A (ZTE CORP.), 07 November 2007 (07.11.2007), the whole document	1-16
A	CN 101621374 A (HUAWEI TECHNOLOGIES CO., LTD.), 06 January 2010 (06.01.2010), the whole document	1-16
A	CN 101815294 A (HUAWEI TECHNOLOGIES CO., LTD.), 25 August 2010 (25.08.2010), the whole document	1-16
A	CN 102447690 A (ZTE CORP.), 09 May 2012 (09.05.2012), the whole document	1-16
A	EP 1872514 A2 (LUCENT TECHNOLOGIES INC.), 02 January 2008 (02.01.2008), the whole document	1-16

☐ Further documents are listed in the continuation of Box C. ☒ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
19 August 2013 (19.08.2013)	**05 September 2013 (05.09.2013)**
Name and mailing address of the ISA/CN: State Intellectual Property Office of the P. R. China No. 6, Xitucheng Road, Jimenqiao Haidian District, Beijing 100088, China Facsimile No.: (86-10) 62019451	Authorized officer **ZHENG, Ning** Telephone No.: (86-10) **62413616**

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/CN2013/076315

Patent Documents referred in the Report	Publication Date	Patent Family	Publication Date
CN 101516090 A	26.08.2009	WO 2009103214 A1	27.08.2009
CN 101141241 A	12.03.2008	WO 2008040196 A1	10.04.2008
		US 2009217032 A1	27.08.2009
CN 101068143 A	07.11.2007	None	
CN 101621374 A	06.01.2010	WO 2010000185 A1	07.01.2010
		US 2011078442 A1	31.03.2011
		EP 2293611 A1	09.03.2011
		KR 2011021945 A	04.03.2011
CN 101815294 A	25.08.2010	None	
CN 102447690 A	09.05.2012	None	
EP 1872514 A2	02.01.2008	WO 2006113189 A2	26.10.2006
		CN 101160778 A	09.04.2008
		KR 20070122490 A	31.12.2007
		US 2006236116 A1	19.10.2006
		JP 2008538482 A	23.10.2008
		IN 200704496 P4	25.01.2008

Form PCT/ISA/210 (patent family annex) (July 2009)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/CN2013/076315

A. CLASSIFICATION OF SUBJECT MATTER

H04L 9/32 (2006.01) i

H04L 9/08 (2006.01) n

Form PCT/ISA/210 (extra sheet) (July 2009)